The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/18/2016

SUBJECT:
A Vulnerability in Cisco Firewall Products Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the Simple Network Management Protocol (SNMP) code of Cisco Firewall products, which could allow for remote code execution. Successful exploitation could allow an unauthenticated user to take control of the affected system and perform unauthorized actions. Failed attempts may result in denial of service conditions.

THREAT INTELLIGENCE:
This vulnerability has been publicly disclosed and a tool exists to perform the exploit. There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco PIX Firewalls
- Cisco Firewall Services Module (FWSM)

All versions of SNMP are affected by this vulnerability.

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:
Cisco firewall products are vulnerable to a buffer overflow affecting the SNMP code, which allows for remote code execution. This vulnerability allows an attacker with knowledge of the device's community string to send maliciously crafted packets to the system and execute code remotely on the system. Failed attempts may crash the device resulting in denial of service conditions.

This vulnerability is associated with stolen exploits and tools taken from the Equation Group. This vulnerability is built into a tool referred to as ExtraBacon which allows for point and click exploitation if all required details are known.

Work Arounds/Mitigating Details:

- Most of the products listed above, which were affected by this vulnerability are End of Life or End of Support. Cisco has indicated that they will be releasing fixes for supported products.
- The attacker must know the device's SNMP community strings in order to successfully launch the attack. Community strings are a password equivalent on Firewall devices to restrict both read-only and read-write access to the SNMP data on the device. Per Cisco, best practices indicate that community strings should be carefully chosen to ensure that they are not trivial, and that should be changed at regular intervals and in accordance with network security policies.
- It is recommended that affected devices are configured to only allow trusted users and hosts to have SNMP access and to monitor these systems using the snmp-server host command.

At this time no patches have been released by Cisco addressing this vulnerability.

RECOMMENDATIONS:
The following actions should be taken:

- Install updates once released by Cisco after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Ensure the enable password is set on the devices in order to prevent privileged access.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:

Cisco:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

XORCat
http://xorcat.net/2016/08/16/equationgroup-tool-leak-extrabacon-demo/

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6366

http://www.us-cert.gov/tlp/